Docket No.: 35997-217836
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Dickerson et al.

Application No.: 09/932,408 | Confirmation No.: 4316

Filed: August 18, 2001 | Art Unit: 2131

For: METHOD AND SYSTEM FOR MAINTAINING SECURE SEMICONDUCTOR DEVICE AREAS | Examiner: L. Chai

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37, this brief is filed more than one month after the Notice of Panel Decision from Pre-Appeal Brief Review issued in this case on January 17, 2006.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

03/20/2006 JADD01 00000029 220261 09932408
01 FC:1402 500.00 DA

I. Real Party In Interest
II Related Appeals and Interferences
III. Status of Claims
IV. Status of Amendments
V. Summary of Claimed Subject Matter
VI. Grounds of Rejection to be Reviewed on Appeal

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Safenet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 24 claims pending in application.

Current Status of Claims

1. Claims canceled: 0

2. Claims withdrawn from consideration but not canceled: 0

3. Claims pending: 1-24

4. Claims allowed: 0

5. Claims rejected: 1-24

B. Claims On Appeal

The claims on appeal are claims 1-24

IV. STATUS OF AMENDMENTS

An Amendment After-Final was filed on August 10, 2005.

The Amendment After-Final incorporated dependent claim 10 into independent claim 1 and dependent claims 17 and 18 into independent claim 13. Claims 10, 17 and 18 were canceled. However, the Examiner declined to enter these amendments as indicated in the Advisory Action of August 24, 2005.

Accordingly, the claims enclosed herein as Appendix A do not incorporate the amendments to claims 1-24, as indicated in the paper filed on August 10, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a method and system for obstructing unauthorized access to security areas of semiconductor devices. The present invention provides numerous advantages over known methods and systems. Advantages of the invention are described in the specification, for example at paragraph 38 among other locations. Advantages of the present invention include preventing users from accessing secure areas of a semiconductor device.

These and other advantages are achievable with the present invention as recited, for example, in independent claim 24. As recited in independent claim 24, the present invention provides a system for obstructing access to a secure area of a semiconductor device. A system includes a microprocessor core 62, please see Figure 4. A decoder 68 may be connected to an output of microprocessor core 62. A control line 69 may be a connected to an output of the decoder 68, please see Figure 4 and paragraph 34. A circuit, such a microprocessor core 62, for supplying output data may be also be provided. A data output line 83 is connected to an output of the circuit for supplying output data. Referring to Figure 5A, an AND gate 82 has a first input 86 connected to the control line 69. A second input 84 of the AND gate 82 is connected to the data output line 83. An output 88 of the AND gate is connected to an input of a buffer 80, see paragraph 34 and Figure 4.

A port 70 is implemented in the semiconductor device 60 for connecting an in-circuit emulator. A line on the port is also connected to an output of the buffer 80, please see paragraph 34 and Figure 4. When the in-circuit emulator requests access to the secure area, the microprocessor core 62 generates microprocessor signals for decoding by the decoder 68. The decoder 68 decodes the microprocessor signals and generates a control signal on the control line 69 connected to the first input 86 of the AND gate 82. The AND gate outputs an obstructing signal to obstruct access by the in-circuit emulator to the secure area, please see paragraphs 36-37 and Figures 4 and 5B.

VI. GROUNDS OF OBJECTION TO BE REVIEWED ON APPEAL

(1) Whether the Examiner has established that claims 2, 4, 5, 10, 11, 17, 18 and 24 are obvious over U.S. Patent Number 6,088,262 to Nasu in view of Applicant admitted prior art publication number U.S. 2003/0212897.

(2) Whether the Examiner has established that claims 1-4, 6-9, 13-16 and 19-23 are anticipated by or in the alternative obvious over U.S. Patent Number 6,088,262 to Nasu.

VII. ARGUMENT

A. The rejection over Nasu in view of AAP

For at least the following reasons, the Action does not establish a prima facie case of obviousness to reject claim 24 based on the combined teachings of Nasu and AAP.

The Final Action refers to the Publication as "AAP," which will be used herein for consistency. Applicants note that the Action also appears to reject claim 24 as being obvious over Nasu in view of AAP (see Final Action, pages 11-13) even though claim 24 is not listed as being rejection in section 11 on page 11 of the Final Action.

Application respectfully traverse this rejection as the Final Action fails to establish a prima facie case of obviousness.

As described above and recited in claim 24, a system according to an embodiment of the invention obstructs access to a secure area of a semiconductor device when an in-circuit emulator requests access to a secure area. Semiconductor devices implementing data encryption typically utilize two modes, a user mode and a supervisor mode. The user mode typically permits the user of the semiconductor device to program the semiconductor device and utilize the functions of the device. However, access to secure internal memory and registers is prohibited when in the user

mode. In supervisor mode, on the other hand, unrestricted access to code, internal and external memory and registers may be provide. An in-circuit emulator may be used to help test the operation of the semiconductor device. However, use of an in-circuit emulator has the draw back that it allows any user to obtain access to the secure areas of the semiconductor device. Consequently, there is a problem with prior art semiconductor devices when used with an in-circuit emulator.

Embodiments of the invention overcome the problems of the prior art by obstructing access to secure areas of the semiconductor device by the in-circuit emulator. For example, referring to Figure 4 and paragraphs 36-38 of the application, when a user issues a command directing the microprocessor core 62 to enter a supervisor mode, the microprocessor core 62 generates signals for decoding by the decoder 68. The decoder 68 decodes the microprocessor signals and generates a control signal on the control line 69. The control signal may transition, from, for example, a high logic state "1" to a low logic state "0". The control signal is provided to an input of the AND gate 82. As long as the control line 69 is in a low logic state, an output 88 of the AND gate 82 will be low and remain low until the user returns to the user mode. Consequently, the AND gate 82 would only output logic "0", thereby obstructing access by the in-circuit emulator to the secure area of the semiconductor device, please see paragraph 37.

Thus, the user who attempts to reads secure areas of the semiconductor device 60 by entering a supervisor mode reads nothing but logic "0". The users' attempts to compromise the secure areas of the semiconductor device 60 are obstructed. The only time a user is able to obtain meaningful data from the semiconductor device 60 is when the user is in the user mode, a mode that does not permit access to the secure access to the secure areas of the semiconductor device, see paragraphs 37 and 38.

For at least the following reasons, the combined teachings of Nasu and AAP do not teach or suggest all of the claim features to render claim 24 obvious under 35 U.S.C. § 103(a).

Neither Nasu nor AAP teach a system that obstructs access to the secure area when an in-circuit emulator requests access to the secure area as recited by the claim 24. Specifically, Nasu and

AAP do not teach or suggest "**when** the in-circuit emulator **requests access to the secure area, the microprocessor core generates** microprocessor signals for decoding by the decoder," "the decoder decodes the microprocessor signals and generates a control signal" provided to an input of the AND gate," the AND gate **outputs an obstructing signal to obstruct access** by the in-circuit emulator **to the secure area**," (emphasis added) as recited in claim 24.

In contrast, AAP teaches that if a user issues a software interrupt (SWI) to direct the microprocessor core 40 to change into a supervisor mode, the secure areas of the semiconductor device 20, such as the supervisor mode memory 44, may be available to the user at port 22, completely defeating the purpose of a secure mode (see AAP, paragraph [0033]). In particular, AAP describes that when a user issues the SWI code to change modes from a user mode to a supervisor mode, support logic 46 decodes signals generated by the microprocessor control 40 and toggles a control signal on control line 50 as shown in Figure 3B of AAP. When, for example, the control signal transitions to a low logical state 54 as a result of the semiconductor device entering the supervisor mode, the secure areas of the semiconductor device 20, such as the supervisor mode memory 44 become enabled, please see paragraph 32. For example, supervisor mode memory and secure registers may be available to the user at ports 22, completely defeating the purpose of a secure mode, please see paragraph 33.

Thus, AAP does not teach or suggest "wherein **when** the in-circuit emulator **requests access** to the secure area, the microprocessor core generates microprocessor signals for decoding by the decoder, and wherein the decoder decodes the microprocessor signals and generates a control signal on the control line connected to the first input of the AND gate, and wherein the AND gate outputs an obstructing signal to **obstruct access** by the in-circuit emulator **to the secure area**," (emphasis added) as recited in claim 24.

Referring now to the teachings of Nasu, similar to AAP, Nasu does not teach or suggest a system that obstructs access by an in-circuit emulator to the secure area, **when** an in-circuit emulator requests access to the secure area as recited in claim 24. On page 13, the Action asserts

that the read protection means described in column 1, lines 55-57 of Nasu teaches this claim feature. Applicants respectfully disagree.

The read protection means of Nasu is further described in column 5, line 5-column 6, line 14. In this section, Nasu teaches a read protection control circuit 107 that may be used to prevent data from being written into or read from a memory cell array 100. Nasu teaches that the read protection control circuit 107 sets the read protection for the memory cell array 100 using the read protection setting signal 117 (see Nasu, col. 5, lines 63-67, also see col. 5, lines 5-18). Nasu teaches that the read protection is set **after** the user of the microcomputer has developed a program and written that program into memory cell array 100 to protect the written program from being copied by third parties (see Nasu, col. 5, line 63-col. 6, line 1).

However, Nasu does not teach or suggest that **when** a third party requests access to the memory cell array 100, access by the third party to the memory cell array 100 is obstructed. In Nasu, if a third party requests access to the memory cell array 100 before the read protection is set, such access is allowed. There is no mechanism described in Nasu to obstruct the access. Thus, Nasu does not teach or suggest "wherein **when** the in-circuit emulator **requests access** to the secure area, the microprocessor core generates microprocessor signals for decoding by the decoder, and wherein the decoder decodes the microprocessor signals and generates a control signal on the control line connected to the first input of the AND gate, and wherein the AND gate outputs an obstructing signal to **obstruct access** by the in-circuit emulator **to the secure area**," (emphasis added) as recited in claim 24. Therefore, the combined teachings of AAP and Nasu do not teach a similar sequence of events occurring **when** an in-circuit emulator **requests access** to a secure area to obstruct access by the in-circuit emulator to the secure area and do not render claim 24 obvious under 35 U.S.C. § 103(a).

Accordingly, claim 24 is allowable over the combined teachings of Nasu and AAP and allowance thereof is respectfully requested. Dependent claim 10 includes similar recitations and is allowable for analogous reasons.

B. The rejection over Nasu

For at least the following reasons, Nasu, does not disclose, teach or suggest all of the features to anticipate or render obvious claims 17 and 18.

Nasu do not teach or suggest "wherein the control signal is utilized by the second circuit to **obstruct access** to the secure area when a mode indicated by the control signal is a secure mode, and wherein the semiconductor device enters the secure mode when the in-circuit emulator is connected to the port," (emphasis added) as recited in claims 17 and 18.

Furthermore, Nasu does not teach or suggest "wherein the control signal is utilized by the second circuit to **obstruct access** to the secure area when a mode indicated by the control signal is a secure mode, and wherein the semiconductor device enters the secure mode when the in-circuit emulator is connected to the port," (emphasis added) as recited in amended claim 13. Nasu does not teach or suggest that the memory cell array 100 enters a secure mode when an in-circuit emulator is connected to a port. Rather, Nasu teaches that after the user of the microcomputer has developed a program and written that program into the memory cell array 100, the read protection is set for the memory cell array 100 (see Nasu, col. 5, lines 64-67). Hence, the secure mode of Nasu is entered when the program is written into the memory cell array 100, and Nasu does not teach or suggest that the memory cell array 100 **enters** the read protection mode **when** a device is attached to a port. Thus, neither AAP nor Nasu teach or suggest "wherein the control signal is utilized by the second circuit to **obstruct access** to the secure area when a mode indicated by the control signal is a secure mode, and wherein the semiconductor device enters the secure mode when the in-circuit emulator is connected to the port," (emphasis added) as recited in amended claim 13. Therefore, Nasu and AAP, alone or in combination, do not anticipate or render obvious claim 13.

Accordingly, claims 17 and 18 are in condition for allowance and allowance thereof is respectfully requested.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE

There has been no evidence pursuant to §§ 1.130, 1.131, or 1.132 or other evidence submitted in this application.

X. RELATED PROCEEDINGS

There are no decisions rendered by a court or the board in this application.

Dated: March 17, 2006

Respectfully submitted,

By _____

Jeffri A. Kaminski
Registration No.: 42,709
James R. Burdett
Registration No.: 31,594
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant

#730527

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/932,408

Claim 1 A method for obstructing access to a secure area of a semiconductor device comprising:

providing a control signal indicating that the semiconductor device has entered a secure mode; and

obstructing access to the secure area utilizing the control signal.

Claim 2 The method of claim 1, wherein obstructing access to the secure area comprises gating another signal with the control signal.

Claim 3 The method of claim 1, wherein obstructing access to the secure area comprises is selecting a multiplexer channel with the control signal.

Claim 4 The method of claim 1, wherein obstructing access to the secure area comprises enabling another circuit with the control signal.

Claim 5 The method of claim 1, wherein the secure area is used in connection with data encryption.

Claim 6 The method of claim 1, wherein providing a control signal further comprises decoding a plurality of signals to generate the control signal.

Claim 7 The method of claim 1, wherein the control signal transitions from a first logic state to a second logic state when the semiconductor device enters the secure mode.

Claim 8 The method of claim 7, wherein the first logic state is a logic high and the second

logic state is a logic low.

Claim 9 The method of claim 7, wherein the first logic state is a logic low and the second logic state is a logic high.

Claim 10 The method of claim 1, further comprising:

connecting an in-circuit emulator to the semiconductor device: and

generating a command from the in-circuit emulator to the semiconductor device, wherein the command requests access to the secure area of the semiconductor.

Claim 11 The method of claim 10, wherein the semiconductor device enters the secure mode when the in-circuit emulator is connected to the semiconductor device.

Claim 12 The method of claim 10, wherein the command is a software interrupt.

Claim 13 A system for obstructing access to a secure area of a semiconductor device comprising:

a first circuit for generating a control signal; and

a second circuit for obstructing access to the secure area connected to the control signal, wherein the control signal is utilized by the second circuit to obstruct access to the secure area when a mode indicated by the control signal is a secure mode.

Claim 14 The system of claim 13, wherein the second circuit is a logic gate.

Claim 15 The system of claim 14, wherein the logic gate is an AND gate having a first input connected to the first circuit such that the first input responds to the control signal;

a second input connected to a circuit supplying output data; and

an output connected to a port of the semiconductor device.

Claim 16 The system of claim 13, wherein the second circuit is a multiplexer.

Claim 17 The system of claim 13, further comprising a port for an in-circuit emulator.

Claim 18 The system of claim 17, wherein the semiconductor device enters the secure mode when the in-circuit emulator is connected to the port.

Claim 19 The system of claim 13, wherein the secure area comprises memory.

Claim 20 The system of claim 13, wherein the semiconductor device is an application specific integrated circuit.

Claim 21 The system of claim 20, wherein the first circuit is a microprocessor core.

Claim 22 They system of claim 13, wherein the first circuit is a decoder.

Claim 23 The system of claim 15, wherein the output is buffered before connecting to the port.

Claim 24 A system for obstructing access to a secure area of a semiconductor device comprising:

a microprocessor core;

a decoder connected to an output of the microprocessor core;

a control line connected to an output of the decoder;

a circuit for supplying output data;

a data output line connected to an output of the circuit for supplying output data; and

an AND gate having a first input connected to the control line, a second input connected to the data output line, and an output connected to an input of a buffer; and

a port implemented in the semiconductor device for connecting to an in-circuit emulator, wherein a line on the port is also connected to an output of the buffer, wherein when the in-circuit

emulator requests access to the secure area, the microprocessor core generates microprocessor signals for decoding by the decoder, and wherein the decoder decodes the microprocessor signals and generates a control signal on the control line connected to the first input of the AND gate, and wherein the AND gate outputs an obstructing signal to obstruct access by the in-circuit emulator to the secure area.

PTO/SB/17 (01-06)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 500.00

Complete if Known	
Application Number	09/932,408-Conf. #4316
Filing Date	August 18, 2001
First Named Inventor	Russell Dickerson
Examiner Name	L. Chai
Art Unit	2131
Attorney Docket No.	35997-217836

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 22-0261 Deposit Account Name: Venable LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

FEE CALCULATION (All the fees below are due upon filing or may be subject to a surcharge.)

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - =	_____ x	_____ =	_____

HP = highest numer of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - =	_____ x	_____ =	_____

HP = highest numer of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ /50	_____ (round up to a whole number) x	_____ =	_____

4. OTHER FEE(S)

	Fees Paid ($)
Other (e.g., late filing surcharge): 1402 Filing a brief in support of an appeal	500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 42,709	Telephone (202) 344-4000
Name (Print/Type)	Jeffri A. Kaminski		Date March 17, 2006

TRANSMITTAL OF APPEAL BRIEF

Docket No. 35997-217836

In re Application of: Dickerson et al.

Application No.	Filing Date	Examiner	Group Art Unit
09/932,408-Conf. #4316	August 18, 2001	L. Chai	2131

Invention: METHOD AND SYSTEM FOR MAINTAINING SECURE SEMICONDUCTOR DEVICE AREAS

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: October 14, 2005 .

The fee for filing this Appeal Brief is $ 500.00 .

[X] Large Entity [ ] Small Entity

[ ] A petition for extension of time is also enclosed.

The fee for the extension of time is _____ .

[ ] A check in the amount of _____ is enclosed.

[X] Charge the amount of the fee to Deposit Account No. 22-0261 .
This sheet is submitted in duplicate.

[ ] Payment by credit card. Form PTO-2038 is attached.

[X] The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 22-0261 .
This sheet is submitted in duplicate.

Dated: March 17, 2006

Jeffri A. Kaminski
Attorney Reg. No. : 42,709
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000